Statement of the Honorable Mary Bono Mack
Chairman, Subcommittee on Commerce, Manufacturing, and Trade
May 4, 2011
Hearing on "The Threat of Data Theft to American Consumers."
(As Prepared for Delivery)

Today, American consumers are under constant assault. As quickly and quietly as a wallet can be stolen by a skilled pickpocket, your personal identity can be hijacked without you knowing it by online hackers. The Federal Trade Commission estimates that nearly nine million Americans fall victim to identity theft every year, costing consumers and businesses billions of dollars annually – and those numbers are growing steadily and alarmingly.

In recent years, sophisticated and carefully orchestrated cyber attacks – designed to obtain personal information about consumers, especially when it comes to their credit cards – have become one of the fastest growing criminal enterprises here in the United States and across the world. The boldness of these attacks and the threat they present to unsuspecting Americans was underscored recently by massive data breaches at Epsilon and Sony.

With 77 million accounts stolen – including some 10 million credit card numbers – the data breach involving Sony's PlayStation Network has the potential to become the "Great Brink's Robbery" of cyber attacks. And the "take" keeps going up.

While the FBI and Secret Service, along with other law enforcement agencies, work around the clock to try and crack this sensational case, we now learn that a second Sony online service was also compromised during the same time period. Computer hackers obtained access to personal information relating to an additional 25 million customer accounts. That's more than 100 million accounts now in jeopardy.

Like their customers, both Sony and Epsilon are victims, too. But they also must shoulder some of the blame for these stunning thefts, which shake the confidence of everyone who types in a credit card number and hits "enter." E-commerce is a vital and growing part of our economy. We should take steps to embrace and protect it – and that starts with robust cyber security.

As Chairman of this Subcommittee, I am deeply troubled by these latest data breaches, and the decision by both Epsilon and Sony not to testify today. This is unacceptable.

According to Epsilon, the company did not have time to prepare for our hearing – even though its data breach occurred more than a month ago. Sony, meanwhile, says it's too busy with its ongoing investigation to appear. Well, what about the millions of American consumers who are still twisting in the wind because of these breaches? They deserve some straight answers, and I am determined to get them.

For instance: How did these breaches occur? What steps are being taken to prevent future breaches? And what's being done to mitigate the effects of these breaches on American consumers?

Yet for me, the single most important question is simply this: Why weren't Sony's customers notified sooner of the cyber attack? I fundamentally believe that all consumers have a right to know when their personal information has been compromised, and Sony – as well as all other companies – have an overriding responsibility to alert them…immediately.

In Sony's case, company officials first revealed information about the data breach on their blog. That's right. A blog. I hate to pile on, but – in essence – Sony put the burden on consumers to "search" for information, instead of accepting the burden of notifying them. If I have anything to do with it, that kind of half-hearted, half-baked response is not going to fly in the future.

This ongoing mess only reinforces my long-held belief that much more needs to be done to protect sensitive consumer information. Americans need additional safeguards to prevent identity theft, and I will soon introduce legislation designed to accomplish this goal. My legislation will be crafted around a guiding principle: Consumers should be promptly informed when their personal information has been jeopardized.

Clearly, cyber attacks are on the rise. According to the Privacy Rights Clearinghouse, over twenty-five hundred data breaches – involving some 600 million records have been made public since 2005. In fact, last month alone, some 30 data breaches at hospitals, insurance companies, universities, banks, airlines and governmental agencies impacted nearly 100 million records. And that's in addition to the massive breaches at Epsilon and Sony.

The time has come for Congress to take decisive action. We need a uniform national standard for data security and data breach notification, and we need it now.

While I remain hopeful that law enforcement officials will quickly determine the extent of these latest cyber attacks, they serves as a reminder – as well as a wake-up call – that all companies have a responsibility to protect personal information and to promptly notify consumers when that information has been put at risk. And we have a responsibility, as lawmakers, to make certain this happens.